PAUL J. ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800

Attorneys for Plaintiff
FINJAN, INC.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

FINJAN, INC., Plaintiff, v. PROOFPOINT, INC. AND ARMORIZE TECHNOLOGIES, INC. Defendants.	Case No.: 5:13-CV-05808-BLF **FIRST SUPPLEMENTAL COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

FIRST SUPPLEMENTAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Finjan, Inc. ("Finjan") files this First Supplemental Complaint for Patent Infringement and Jury Demand against Defendants Proofpoint, Inc. ("Proofpoint") and Armorize Technologies, Inc. ("Armorize"), (collectively "Defendants") and alleges as follows:

THE PARTIES

1. Finjan is a Delaware corporation, with its principal place of business at 333 Middlefield Road, Suite 110, Menlo Park, CA 94025. Finjan's U.S. operating business was previously headquartered at 2025 Gateway Place, San Jose, California 95110.

2. Proofpoint is a Delaware corporation with its principal place of business at 892 Ross Drive, Sunnyvale, California 94089.

3. Armorize is a Delaware corporation with its principal place of business at 892 Ross Drive, Sunnyvale, California 94089. Armorize is a wholly-owned subsidiary of Proofpoint.

JURISDICTION AND VENUE

4. This action arises under the Patent Act, 35 U.S.C. § 101 *et seq*. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

5. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b) and (c) and/or 1400(b).

6. This Court has personal jurisdiction over Defendants. Upon information and belief, Defendants do business in this District and has, and continue to, infringe and/or induce the infringement in this District. Defendants also market their products primarily in and from this District. In addition, the Court has personal jurisdiction over Defendants because they have established minimum contacts with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

FINJAN'S INNOVATIONS

7. Finjan was founded in 1997 as a wholly-owned subsidiary of Finjan Software Ltd., an Israeli corporation. Finjan was a pioneer in the developing proactive security technologies capable of detecting previously unknown and emerging online security threats recognized today under the umbrella of "malware." These technologies protect networks and endpoints by identifying suspicious patterns and behaviors of content delivered over the Internet. Finjan has been awarded, and continues to prosecute, numerous patents in the United States and around the world resulting directly from Finjan's more than decade-long research and development efforts, supported by a dozen inventors.

8. Finjan built and sold software, including APIs, and appliances for network security using these patented technologies. These products and customers continue to be supported by Finjan's licensing partners. At its height, Finjan employed nearly 150 employees around the world building and selling security products and operating the Malicious Code Research Center through which it frequently published research regarding network security and current threats on the Internet. Finjan's pioneering approach to online security drew equity investments from two major software and technology companies, the first in 2005, followed by the second in 2006. Through 2009, Finjan has generated millions of dollars in product sales and related services and support revenues.

9. Finjan's founder and original investors are still involved with and invested in the company today, as are a number of other key executives and advisors. Currently, Finjan is a technology company applying its research, development, knowledge and experience with security technologies to working with inventors, investing in and/or acquiring other technology companies, investing in a variety of research organizations, and evaluating strategic partnerships with large companies.

10. On June 6, 2006, U.S. Patent No. 7,058,822 ("the '822 Patent"), entitled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll and Shlomo Touboul. A true and correct copy of the '822 Patent is attached to this First Supplemental Complaint as Exhibit A and is incorporated by reference herein.

11. All rights, title, and interest in the '822 Patent have been assigned to Finjan, who is the sole owner of the '822 Patent. Finjan has been the sole owner of the '822 Patent since its issuance.

12. The '822 Patent is generally directed towards computer networks and more particularly provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by determining whether any part of such web-based content can be executed and then trapping such content and neutralizing possible harmful effects using mobile protection code. Additionally, the system provides a way to analyze such web-content to determine whether it can be executed.

13. On January 12, 2010, U.S. Patent No. 7,647,633 ("the '633 Patent"), entitled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll and Shlomo Touboul. A true and correct copy of the '633 Patent is attached to this First Supplemental Complaint as Exhibit B and is incorporated by reference herein.

14. All rights, title, and interest in the '633 Patent have been assigned to Finjan, who is the sole owner of the '633 Patent. Finjan has been the sole owner of the '633 Patent since its issuance.

15. The '633 Patent is generally directed towards computer networks, and more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by determining whether

any part of such web-based content can be executed and then trapping such content and neutralizing possible harmful effects using mobile protection code.

16. On November 28, 2000, U.S. Patent No. 6,154,844 ("the '844 Patent"), entitled SYSTEM AND METHOD FOR ATTACHING A DOWNLOADABLE SECURITY PROFILE TO A DOWNLOADABLE, was issued to Shlomo Touboul and Nachshon Gal. A true and correct copy of the '844 Patent is attached to this Complaint as Exhibit C and is incorporated by reference herein.

17. All rights, title, and interest in the '844 Patent have been assigned to Finjan, who is the sole owner of the '844 Patent. Finjan has been the sole owner of the '844 Patent since its issuance.

18. The '844 Patent is generally directed towards computer networks, and more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by linking a security profile to such web-based content to facilitate the protection of computers and networks from malicious web-based content.

19. On July 5, 2011, U.S. Patent No. 7,975,305 ("the '305 Patent"), entitled METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS FOR DESKTOP COMPUTERS, was issued to Moshe Rubin, Moshe Matitya, Artem Melnick, Shlomo Touboul, Alexander Yermakov and Amit Shaked. A true and correct copy of the '305 Patent is attached to this First Supplemental Complaint as Exhibit D and is incorporated by reference herein.

20. All rights, title, and interest in the '305 Patent have been assigned to Finjan, who is the sole owner of the '305 Patent. Finjan has been the sole owner of the '305 Patent since its issuance.

21. The '305 Patent is generally directed towards network security and, in particular, rule-based scanning of web-based content for exploits. One of the ways this is accomplished is by using

parser and analyzer rules to describe computer exploits as patterns of types of tokens. Additionally, the system provides a way to keep these rules updated.

22. On July 17, 2012, U.S. Patent No. 8,225,408 ("the '408 Patent"), entitled METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS, was issued to Moshe Rubin, Moshe Matitya, Artem Melnick, Shlomo Touboul, Alexander Yermakov and Amit Shaked. A true and correct copy of the '408 Patent is attached to this First Supplemental Complaint as Exhibit E and is incorporated by reference herein.

23. All rights, title, and interest in the '408 Patent have been assigned to Finjan, who is the sole owner of the '408 Patent. Finjan has been the sole owner of the '408 Patent since its issuance.

24. The '408 Patent is generally directed towards network security and, in particular, rule-based scanning of web-based content for a variety of exploits written in different programming languages. One of the ways this is accomplished is by expressing the exploits as patterns of tokens. Additionally, the system provides a way to analyze these exploits by using a parse tree.

25. On December 13, 2011, U.S. Patent No. 8,079,086 ("the '086 Patent"), entitled MALICIOUS MOBILE CODE RUNETIME MONITORING SYSTEM AND METHODS, was issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R Kroll and Shlomo Touboul. A true and correct copy of the '086 Patent is attached to this First Supplemental Complaint as Exhibit F and is incorporated herein.

26. All rights, title, and interest in the '086 Patent have been assigned to Finjan, who is the sole owner of the '086 Patent. Finjan has been the sole owner of the '086 Patent since its issuance.

27. The '086 Patent is generally directed towards computer networks and, more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by creating a profile of

the web-based content and sending these profiles and corresponding web-content to another computer for appropriate action.

28. On March 20, 2012, U.S. Patent No. 8,141,154 ("the '154 Patent"), entitled SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE, was issued to David Gruzman and Yuval Ben-Itzhak. On February 25, 2014, the USPTO issued a Certificate of Correction clarifying the priority date for the '154 Patent. A true and correct copy of the '154 Patent, including the Certificate of Correction, is attached to this First Supplemental Complaint as Exhibit G and is incorporated by reference herein.

29. All rights, title, and interest in the '154 Patent have been assigned to Finjan, who is the sole owner of the '154 Patent. Finjan has been the sole owner of the '154 Patent since its issuance.

30. The '154 Patent is generally directed towards a gateway computer protecting a client computer from dynamically generated malicious content. One way this is accomplished is to use a content processor to process a first function and invoke a second function if a security computer indicates that it is safe to invoke the second function.

31. On November 3, 2009, U.S. Patent No. 7,613,918 ("the '918 Patent"), entitled SYSTEM AND METHOD FOR ENFORCING A SECURITY CONTEXT ON A DOWNLOADABLE, was issued to Yuval Ben-Itzhak. A true and correct copy of the '918 Patent is attached to this First Supplemental Complaint as Exhibit H and is incorporated by reference herein.

32. All rights, title, and interest in the '918 Patent have been assigned to Finjan, who is the sole owner of the '918 Patent. Finjan has been the sole owner of the '918 Patent since its issuance.

33. The '918 Patent is generally directed to a system and method for enforcing a security context on a Downloadable. One way this is accomplished is by making use of security contexts that

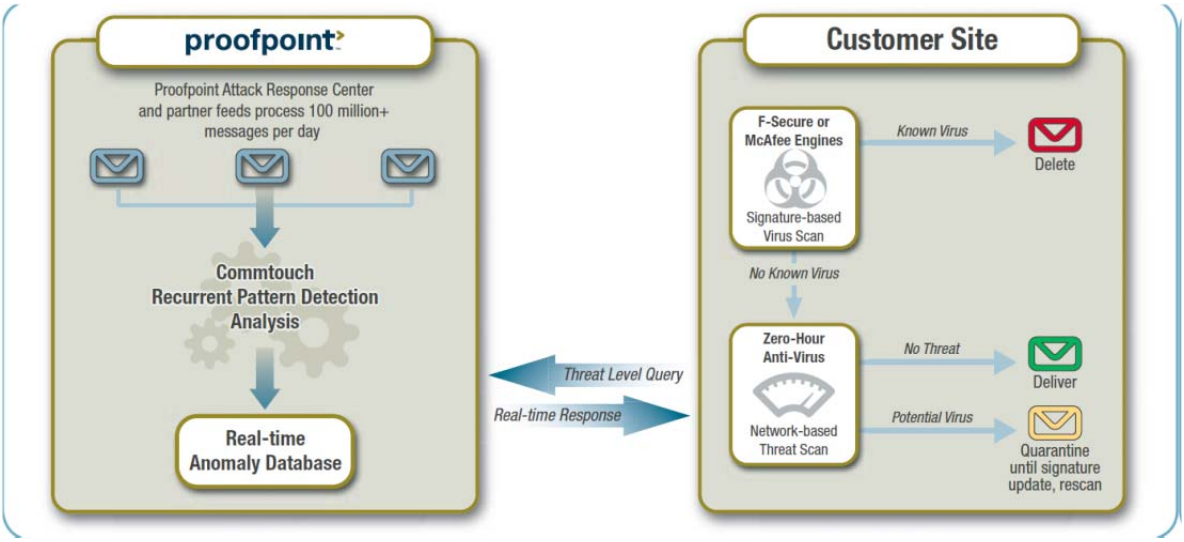
are associated within certain user/group computer accounts when deriving a profile for code received from the Internet.

PROOFPOINT AND ARMORIZE

34. Proofpoint is a security as a service ("SaaS") vendor that delivers data protection solutions to help organizations protect data from attacks and enable clients to meet regulatory compliance and data governance mandates.

35. Proofpoint uses, sells, offers for sale, and/or imports into the United States and this District products and services that utilize Proofpoint's Zero-Hour Threat Detection, Malware Analysis Service and Targeted Attack Protection, including but not limited to the following: Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection Server, and Proofpoint Messaging Security Gateway.

36. Proofpoint's Zero-Hour Threat Detection works with other Proofpoint defense products. First, messages are scanned for policy violations and then scanned by traditional anti-virus defenses. After traditional anti-virus declares a message clean, it is then sent to the Zero-Hour module, which analyzes incoming messages for similarities with suspected virus messages. Messages and attachments that exhibit recurrent pattern characteristics of the emerging virus are automatically quarantined. The Zero-Hour module determines whether a message has a medium or high possibility of being infected by a virus. These messages are delayed in quarantine for a period of time. This process is shown below:

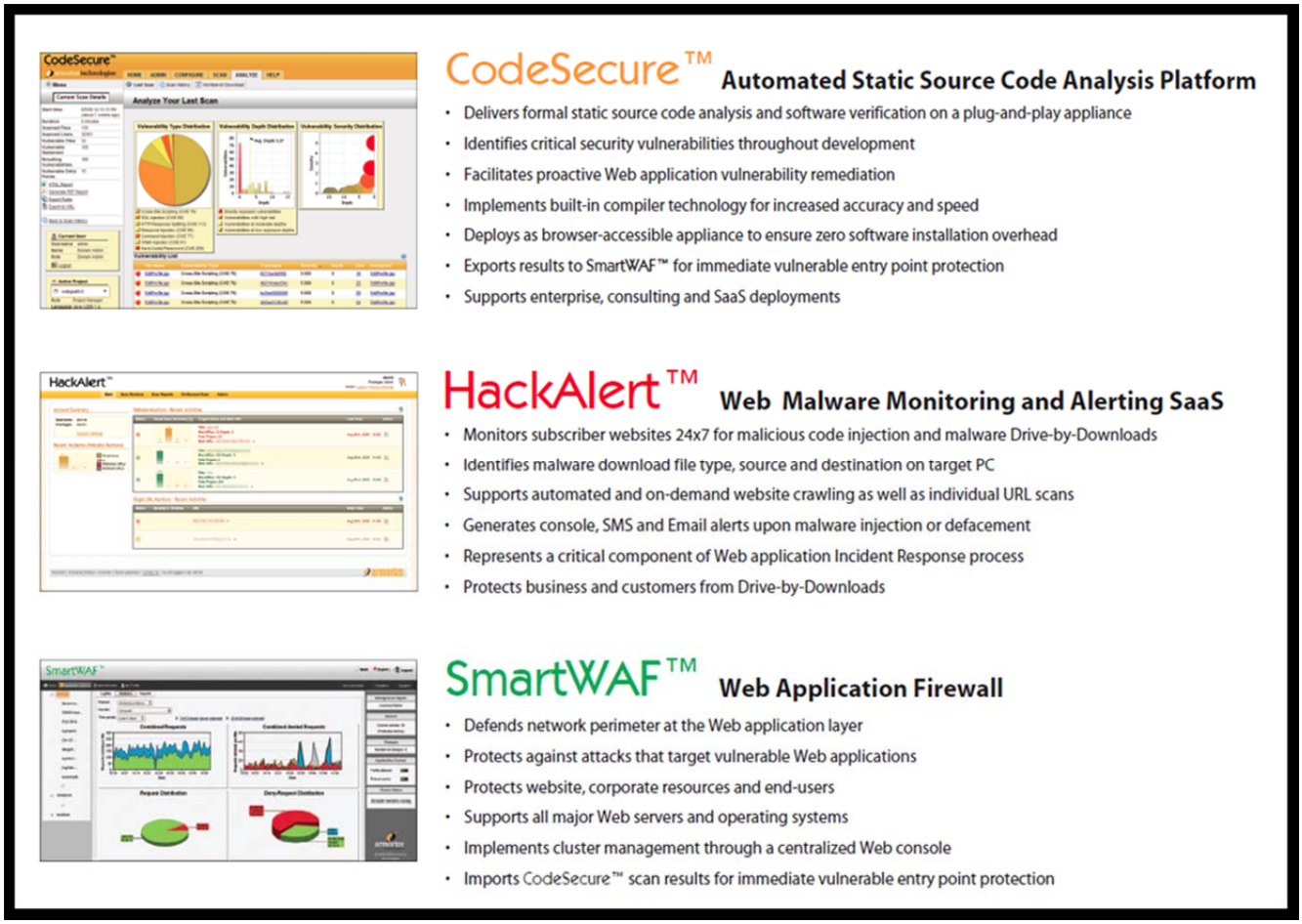


See WP-Proofpoint-Close-the-Zero-Hour-Gap (attached as Exhibit I).

37. Proofpoint's Targeted Attack Protection and Malware Analysis Service (also known as Next Generation Detection) allow unknown malicious attacks that are missed by traditional signature based detection to be caught. Proofpoint's Malware Analysis Service utilizes anomalytics to identify suspicious files and begins the process of analyzing the files in a sandbox for signs of a malware attack. DS-Proofpoint-Targeted-Attack-Protection (attached as Exhibit J).

38. On September 5, 2013, a wholly-owned subsidiary of Proofpoint merged with and into Armorize Technologies, Inc. ("Armorize"), with Armorize surviving as a wholly-owned subsidiary of Proofpoint. Armorize develops and markets SaaS anti-malware products and real-time dynamic detection of next generation threats. Proofpoint Form 10-Q (attached as Exhibit K).

39. Proofpoint paid $25,000,000 in cash for Armorize and has been utilizing Armorize technologies in Proofpoint's products for nearly a year before the acquisition. *See* Proofpoint, Inc. to Acquire Armorize Technologies, Inc.pdf (attached as Exhibit L). Armorize products include HackAlert Anti-Malware, CodeSecure Automated Static Source Code Analysis and SmartWAF Web Application Firewall. Information concerning these products is shown below:



See Armorize Technologies End-to-End Web Application Security (attached as Exhibit M).

40. Armorize, now integrated into Proofpoint, uses, sells, offers for sale, and/or imports into the United States and this District products and services that utilize HackAlert Anti-Malware, CodeSecure Automated Static Source Code Analysis and SmartWAF Web Application Firewall, including but not limited to the following: HackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, HackAlert CodeSecure, HackAlert Vulnerability Assessment and SmartWAF.

41. HackAlert is a service that analyzes, detects, prevents, and mitigates malware infections in online advertisements, documents and e-mails. HackAlert focuses on scanning for zero-day malware and exploits used in Advanced Persistent Threat ("APT") attacks, which are undetectable by typical virus or malware scanners. HackAlert's sandbox analyzes these zero-day exploits and APT, such as malicious binaries, document exploits (PDF, Word, Excel, PowerPoint, Flash), Java exploits, browser exploits, drive-by downloads and click-to downloads. *See* Take APT Malware By Storm (attached as Exhibit N).

42. CodeSecure is an automatic static code analysis platform that identifies security vulnerabilities and works with SmartWAF and HackAlert to provide vulnerability entry point protection. CodeSecure identifies vulnerabilities such as Cross Site Scripting, File Inclusion, Malicious File Execution, Information Leakage and SQL Injection. CodeSecure checks for vulnerabilities based on algorithms to determine behavior outcomes of input data. *See* CodeSecure (attached as Exhibit O).

43. SmartWAF is a web application firewall. It defends against web application attacks such as SQL Injection, Cross Site Scripting, Cross Site Request Forgery, Cookie Tampering, Directory Indexing, Information Leakage, Content Spoofing, Application Fingerprinting and Web Server Fingerprinting. SmartWAF may also integrate with CodeSecure by importing source code analysis findings and reconfiguring its rule set to block web application exploits targeted at vulnerabilities identified by CodeSecure.

44. Armorize deploys a developers' API for HackAlert Scanning and Forensics Extraction for Malware. With the API, developers can detect malware not normally caught by normal anti-virus technologies, such as zero-day exploits or Advanced Persistent Threats; automatically induce malware behavior and collect forensics information; and scan individual URLs for Web malware,

such as drive-by downloads and click-to downloads, and generate trackbacks, exploitation steps, JavaScript execution and malware execution. *See* APT-malware-malvertising-scanning-api (attached as Exhibit P).

DEFENDANT'S INFRINGEMENT OF FINJAN'S PATENTS

45. Defendants have been and are now infringing the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent, the '154 Patent and the '918 Patent (collectively "the Patents-In-Suit") in this judicial District, and elsewhere in the United States by, among other things, making, using, importing, selling, and/or offering for sale the claimed systems and methods that utilize Proofpoint's Zero-Hour Threat Detection, Proofpoint's Malware Analysis Service, Proofpoint's Targeted Attack Protection, HackAlert, and CodeSecure, including without limitation on Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials, Proofpoint Protection Server, Proofpoint Messaging Security GatewayHackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, HackAlert CodeSecure, HackAlert Vulnerability Assessment and SmartWAF.

46. In addition to directly infringing the Patents-In-Suit pursuant to 35 U.S.C. § 271(a) either literally or under the doctrine of equivalents, Defendants indirectly infringe the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent and the '918 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its users and developers, to perform all or some of the steps of method claims of the Patents-In-Suit, either literally or under the doctrine of equivalents.

COUNT I
(Direct Infringement of the '822 Patent pursuant to 35 U.S.C. § 271(a))

47. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

48. Defendants have infringed and continue to infringe one or more claims of the '822 Patent in violation of 35 U.S.C. § 271(a).

49. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

50. Defendants' acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

51. Defendants' infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendants' products and services, including but not limited to HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection, which embody the patented invention of the '822 Patent.

52. As a result of Defendants' unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

53. Defendants' infringement of the '822 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT II
(Indirect Infringement of the '822 Patent pursuant to 35 U.S.C. § 271(b))

54. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

55. Defendants have induced and continue to induce infringement of at least claims 1-3, 4-8, and 16-27 of the '822 Patent under 35 U.S.C. § 271(b).

56. In addition to directly infringing the '822 Patent, Defendants indirectly infringe the '822 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to its customers, users and developers, to perform all or some of the steps of the

method claims, either literally or under the doctrine of equivalents, of the '822 Patent, where all the steps of the method claims are performed by either Defendants or their customers, users or developers, or some combination thereof. Defendants have known or have been willfully blind to the fact that they are inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '822 Patent.

57. Defendants knowingly and actively aid and abet the direct infringement of the '822 Patent by instructing and encouraging their customers, users and developers to use the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection. Such instructions and encouragement include, but are not limited to, advising third parties to use the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection in an infringing manner; providing a mechanism through which third parties may infringe the '822 Patent, specifically through the use of the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection; advertising and promoting the use of the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection in an infringing manner; and distributing guidelines and instructions to third parties on how to use the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection in an infringing manner.

58. Defendants provide detailed instructions to their customers and users regarding all aspects of the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection, including HackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, HackAlert Vulnerability Assessment, Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection Server, and Proofpoint Messaging Security

Gateway. Examples of these instructions can be found at the Armorize Resource Center (at http://armorize.com/index.php?link_id=product), Armorize Forums / Tutorials, FAQs (at https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources), and Proofpoint Resources (at http://www.proofpoint.com/resources/index.php).

59. Proofpoint itself and through its authorized partners regularly provides classroom style training, demonstrations, webinars, and certification programs to help users use Proofpoint Targeted Attack Protection and Malware Analysis Service, including without limitation the following:

- Webinars on Contextual Security Approach to Protection From Targeted Threats, Undetected Threats: Finding and protecting against hundreds of missed attacks, Combatting 2013's Most Dangerous Attacks, and Spearing the Spear Phishers: How to Reliably Defeat Targeted Attacks. *See* http://www.proofpoint.com/resources/webinars.php (attached as Exhibit Q);

- Demonstrations including Proofpoint Integrated Product Suite Demo and Proofpoint Enterprise Protection Live Demo. The demonstrations show how to use the Targeted Attack Protection to protect organizations. *See* http://www.proofpoint.com/resources/demos.php (attached as Exhibit R);

- Technical Briefs on Proofpoint Zero-Hour Anti-Virus and White Papers on Targeted Attack: The Best Defense, Defense against the Dark Arts: Finding and Stopping Advanced Threats, and Longline Phishing: A New Class of Advanced Phishing Attacks. *See* http://www.proofpoint.com/resources/white-papers.php (attached as Exhibit S);

- Proofpoint Education Portal which offers courses in Enterprise Protection Accredited Engineer, Enterprise Protection Suite, Enterprise Protection for the Administrator, Proofpoint Targeted Attack Protection for End Users, Staying Safe on Email, and Enterprise Protection Associate Level Training. *See* http://www.training.proofpoint.com/courses-draft/ (attached as Exhibit T);

- Proofpoint Education Portal which offers On-Site Training where a group of up to 8 people can be trained live by Proofpoint to use their Protection products. *See* http://www.training.proofpoint.com/classroom-schedule/on-site/ (attached as Exhibit U).

60. Proofpoint offers Professional Services, which helps customers design and implement Proofpoint's products onto the customers' network. Professional Services also offers integration, customization, training and maintenance of Proofpoint's products.

61. Armorize posts tutorials, user guides, troubleshooting and explanations on its online forum on how to use Armorize technology. These include without limitation HackAlert Resources, HackAlert SafeImpression question documents, tutorials on what to do "when a drive-by-download knocks at your door," tutorial on "How to add a website into HackAlert to be monitored," and tutorial on "what to do when receiving an alert." *See* https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources (attached as Exhibit V).

62. Armorize provides the HackAlert V5 API, which encourages developers and customers to use HackAlert with step-by-step instructions on how to integrate into the HackAlert Software. *See* Armorize Malware Scanning and Forensics Extraction API (attached as Exhibit P).

63. Defendants actively and intentionally maintains and updates websites, including Proofpoint.com and Armorize.com, to promote and provide demonstration, instruction and technical assistance for the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection products, and to encourage customers, users and developers to use the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection products and practice the methods taught in the '822 Patent.

64. Defendants have had knowledge of the '822 Patent at least as of the time they learned of this action for infringement, and by continuing their actions described above, Defendants have had the specific intent to or were willfully blind to the fact that their actions would induce infringement of the '822 Patent.

COUNT III

(Direct Infringement of the '633 Patent pursuant to 35 U.S.C. § 271(a))

65. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

66. Defendants have infringed and continue to infringe one or more claims of the '633 Patent in violation of 35 U.S.C. § 271(a).

67. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

68. Defendants' acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

69. Defendants' infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendants' products and services, including but not limited to the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection, which embody the patented invention of the '633 Patent.

70. As a result of Defendants' unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

71. Defendants' infringement of the '633 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT IV
(Indirect Infringement of the '633 Patent pursuant to 35 U.S.C. §§ 271(b))

72. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

73. Defendants have induced and continue to induce infringement of at least claims 1-7 and 28-33 of the '633 Patent under 35 U.S.C. § 271(b).

74. In addition to directly infringing the '633 Patent, Defendants indirectly infringe the '633 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to its customers, users and developers, to perform all or some of the steps of the

method claims, either literally or under the doctrine of equivalents, of the '633 Patent, where all the steps of the method claims are performed by either Defendants or their customers, users or developers, or some combination thereof. Defendants have known or have been willfully blind to the fact that they are inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '633 Patent.

75. Defendants knowingly and actively aid and abet the direct infringement of the '633 Patent by instructing and encouraging their customers, users and developers to use the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection. Such instructions and encouragement include but are not limited to, advising third parties to use HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection in an infringing manner; providing a mechanism through which third parties may infringe the '633 Patent, specifically through the use of HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection; advertising and promoting the use of HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection in an infringing manner; and distributing guidelines and instructions to third parties on how to use HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection in an infringing manner.

76. Defendants provide detailed instruction to its customers and users regarding all aspects of the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection including, HackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, HackAlert Vulnerability Assessment, Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection Server, and Proofpoint Messaging Security

Gateway. Examples of these instructions can be found at the Armorize Resource Center located at http://armorize.com/index.php?link_id=product, Armorize Forums / Tutorials, FAQs (at https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources), and Proofpoint Resources (at http://www.proofpoint.com/resources/index.php).

77. Proofpoint itself and through its authorized partners regularly provides class-room style training, demonstrations, webinars, and certification programs to help users use Proofpoint Targeted Attack Protection and Malware Analysis Service, including without limitation the following:

- Webinars on Contextual Security Approach to Protection From Targeted Threats, Undetected Threats: Finding and protecting against hundreds of missed attacks, Combatting 2013's Most Dangerous Attacks, and Spearing the Spear Phishers: How to Reliably Defeat Targeted Attacks. *See* http://www.proofpoint.com/resources/webinars.php (attached as Exhibit Q);

- Demonstrations including Proofpoint Integrated Product Suite Demo and Proofpoint Enterprise Protection Live Demo. The demonstrations show how to use the Targeted Attack Protection to protect organizations. *See* http://www.proofpoint.com/resources/demos.php (attached as Exhibit R);

- Technical Briefs on Proofpoint Zero-Hour Anti-Virus and White Papers on Targeted Attack: The Best Defense, Defense against the Dark Arts: Finding and Stopping Advanced Threats, and Longline Phishing: A New Class of Advanced Phishing Attacks. *See* http://www.proofpoint.com/resources/white-papers.php (attached as Exhibit S);

- Proofpoint Education Portal, which offers courses in Enterprise Protection Accredited Engineer, Enterprise Protection Suite, Enterprise Protection for the Administrator, Proofpoint Targeted Attack Protection for End Users, Staying Safe on E-mail, and Enterprise Protection Associate Level Training. *See* http://www.training.proofpoint.com/courses-draft/ (attached as Exhibit T);

- Proofpoint Education Portal which offers On-Site Training where a group of up to 8 people can be trained live by Proofpoint to use their Protection products. *See* http://www.training.proofpoint.com/classroom-schedule/on-site/ (attached as Exhibit U).

78. Proofpoint offers Professional Services, which helps customers design and implement Proofpoint's products onto the customers' network. Professional Services also offers integration, customization, training and maintenance of Proofpoint's products.

79. Armorize posts tutorials, user guides, troubleshooting and explanations on its online forum on how to use Armorize technology. These include without limitation HackAlert Resources, HackAlert SafeImpression question documents, tutorials on what to do "when a drive-by-download knocks at your door," tutorial on "How to add a website into HackAlert to be monitored," and tutorial on "what to do when receiving an alert." *See* https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources (attached as Exhibit V).

80. Armorize provides the HackAlert V5 API, which encourages developers and customers to use HackAlert with step-by-step instructions on how to integrate into the HackAlert Software. *See* Armorize Malware Scanning and Forensics Extraction API (attached as Exhibit P).

81. Defendants actively and intentionally maintain and update their websites, including Proofpoint.com and Armorize.com, to promote and provide demonstration, instruction and technical assistance for the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection products, and to encourage customers, users and developers to use the HackAlert, Proofpoint Malware Analysis Service, and Proofpoint Targeted Attack Protection products and practice the methods taught in the '633 Patent.

82. Defendants have had knowledge of the '633 Patent at least as of the time they learned of this action for infringement, and by continuing the actions described above, Defendants have had the specific intent to or was willfully blind to the fact that their actions would induce infringement of the '633 Patent.

COUNT V
(Direct Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(a))

83. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

84. Proofpoint has infringed and continues to infringe one or more claims of the '844 Patent in violation of 35 U.S.C. § 271(a).

85. Proofpoint's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

86. Proofpoint's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

87. Proofpoint's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Proofpoint's products and services, including but not limited to Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection, which embodies the patented invention of the '844 Patent.

88. As a result of Proofpoint's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

89. Proofpoint's infringement of the '844 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT VI
(Indirect Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(b))

90. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

91. Proofpoint has induced and continues to induce infringement of at least claims 1-14 and 22-27 of the '844 Patent under 35 U.S.C. § 271(b).

92. In addition to directly infringing the '844 Patent, Proofpoint indirectly infringes the '844 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to its customers, users and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '844 Patent, where all the steps of the method claims are performed by either Proofpoint or its customers, users or developers, or some combination thereof. Proofpoint has known or has been willfully blind to the fact that it is inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Proofpoint, one or more method claims of the '844 Patent.

93. Proofpoint knowingly and actively aids and abets the direct infringement of the '844 Patent by instructing and encouraging its customers, users and developers to use the Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection. Such instructions and encouragement include but are not limited to, advising third parties to use the Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection in an infringing manner; providing a mechanism through which third parties may infringe the '844 Patent, specifically through the use of the Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection; advertising and promoting the use of the Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection in an infringing manner; and distributing guidelines and instructions to third parties on how to use the Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection in an infringing manner.

94. Proofpoint provides detailed instructions to its customers and users regarding all aspects of the Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection including, Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection

Server, and Proofpoint Messaging Security Gateway. Examples of these instructions can be found at the Proofpoint Resources located at http://www.proofpoint.com/resources/index.php.

95. Proofpoint itself and through its authorized partners regularly provides class-room style training, demonstrations, webinars, and certification programs to help users use Proofpoint Targeted Attack Protection and Malware Analysis Service, including without limitation the following:

- Webinars on Contextual Security Approach to Protection From Targeted Threats, Undetected Threats: Finding and protecting against hundreds of missed attacks, Combatting 2013's Most Dangerous Attacks, and Spearing the Spear Phishers: How to Reliably Defeat Targeted Attacks. *See* http://www.proofpoint.com/resources/webinars.php (attached as Exhibit Q);

- Demonstrations includingProofpoint Integrated Product Suite Demo and Proofpoint Enterprise Protection Live Demo. The demonstrations show how to use the Targeted Attack Protection to protect organizations. *See* http://www.proofpoint.com/resources/demos.php (attached as Exhibit R);

- Technical Briefs on Proofpoint Zero-Hour Anti-Virus and White Papers on Targeted Attack: The Best Defense, Defense against the Dark Arts: Finding and Stopping Advanced Threats, and Longline Phishing: A New Class of Advanced Phishing Attacks. *See* http://www.proofpoint.com/resources/white-papers.php (attached as Exhibit S);

- Proofpoint Education Portal, which offers courses in Enterprise Protection, Accredited Engineer, Enterprise Protection Suite, Enterprise Protection for the Administrator, Proofpoint Targeted Attack Protection for End Users, Staying Safe on E-mail, and Enterprise Protection Associate Level Training. *See* http://www.training.proofpoint.com/courses-draft/ (attached as Exhibit T);

- Proofpoint Education Portal which offers On-Site Training where a group of up to 8 people can be trained live by Proofpoint to use their Protection products. *See* http://www.training.proofpoint.com/classroom-schedule/on-site/ (attached as Exhibit U).

96. Proofpoint offers Professional Services, which helps customers design and implement Proofpoint's products onto the customers' network. Professional Services also offers integration, customization, training and maintenance of Proofpoint's products.

97. Proofpoint actively and intentionally maintains and updates websites, including Proofpoint.com, to promote and provide demonstration, instruction and technical assistance for the Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection, and to encourage customers, users and developers to use Proofpoint Malware Analysis Service and Proofpoint Targeted Attack Protection and practice the methods taught in the '844 Patent.

98. Proofpoint has had knowledge of the '844 Patent at least as of the time it learned of this action for infringement, and by continuing the actions described above, Proofpoint has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '844 Patent.

COUNT VII
(Direct Infringement of the '305 Patent pursuant to 35 U.S.C. § 271(a))

99. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

100. Defendants have infringed and continue to infringe one or more claims of the '305 Patent in violation of 35 U.S.C. § 271(a).

101. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

102. Defendants' acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

103. Defendants' infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendants' products and services, including but not limited to, Proofpoint Zero-Hour and CodeSecure, which embody the patented invention of the '305 Patent.

104. As a result of Defendants' unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

105. Defendants' infringement of the '305 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT VIII
(Indirect Infringement of the '305 Patent pursuant to 35 U.S.C. § 271(b))

106. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

107. Defendants have induced and continues to induce infringement of at least claims 13-24, of the '305 Patent under 35 U.S.C. § 271(b).

108. In addition to directly infringing the '305 Patent, Defendants indirectly infringe the '305 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to their customers, users and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '305 Patent, where all the steps of the method claims are performed by either Defendants or their customers, users or developers, or some combination thereof. Defendants have known or have been willfully blind to the fact that they are inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '305 Patent.

109. Defendants knowingly and actively aid and abet the direct infringement of the '305 Patent by instructing and encouraging their customers, users and developers to use Proofpoint Zero-Hour and CodeSecure. Such instructions and encouragement include but are not limited to, advising third parties to use Proofpoint Zero-Hour and CodeSecure in an infringing manner; providing a

mechanism through which third parties may infringe the '305 Patent, specifically through the use of the Proofpoint Zero-Hour and CodeSecure; advertising and promoting the use of the Proofpoint Zero-Hour and CodeSecure in an infringing manner; and distributing guidelines and instructions to third parties on how to use the Proofpoint Zero-Hour and CodeSecure in an infringing manner.

110. Defendants provide detailed instruction to their customers and users regarding all aspects of the Proofpoint Zero-Hour and CodeSecure. Examples of these instructions can be found at the Armorize Resource Center located at http://armorize.com/index.php?link_id=product, Armorize Forums / Tutorials, FAQs (at https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources), and Proofpoint Resources (at http://www.proofpoint.com/resources/index.php).

111. Proofpoint itself and through its authorized partners regularly provides class-room style training, demonstrations, webinars, and certification programs to help users use Proofpoint Targeted Attack Protection and Malware Analysis Service including without limitation the following:

- Webinars on Contextual Security Approach to Protection From Targeted Threats, Undetected Threats: Finding and protecting against hundreds of missed attacks, Combatting 2013's Most Dangerous Attacks, and Spearing the Spear Phishers: How to Reliably Defeat Targeted Attacks. *See* http://www.proofpoint.com/resources/webinars.php (attached as Exhibit Q);

- Demonstrations including Proofpoint Integrated Product Suite Demo and Proofpoint Enterprise Protection Live Demo. The demonstrations show how to use the Targeted Attack Protection to protect organizations. *See* http://www.proofpoint.com/resources/demos.php (attached as Exhibit R);

- Technical Briefs on Proofpoint Zero-Hour Anti-Virus and White Papers on Targeted Attack: The Best Defense, Defense against the Dark Arts: Finding and Stopping Advanced Threats, and Longline Phishing: A New Class of Advanced Phishing Attacks. *See* http://www.proofpoint.com/resources/white-papers.php (attached as Exhibit S);

- Proofpoint Education Portal, which offers courses in Enterprise Protection, Accredited Engineer, Enterprise Protection Suite, Enterprise Protection for the Administrator, Proofpoint Targeted Attack Protection for End Users, Staying Safe on E-mail, and Enterprise Protection Associate Level Training. *See* http://www.training.proofpoint.com/courses-draft/ (attached as Exhibit T);

- Proofpoint Education Portal which offers On-Site Training where a group of up to 8 people can be trained live by Proofpoint to use their Protection products. *See* http://www.training.proofpoint.com/classroom-schedule/on-site/ (attached as Exhibit U).

112. Proofpoint offers Professional Services, which helps customers design and implement Proofpoint's products onto the customers network. Professional Services also offers integration, customization, training and maintenance of Proofpoint's products.

113. Armorize posts tutorials, user guides, troubleshooting and explanations on its online forum on how to use Armorize technology. These include without limitation documents on Code Secure Quick Start Guides, How to upgrade CodeSecure, and LDAP integration tip with CodeSecure. *See* https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources (attached as Exhibit V).

114. Defendants actively and intentionally maintain and update websites, including Proofpoint.com and Armorize.com, to promote and provide demonstration, instruction and technical assistance for HackAlert Code Secure, Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection Server, and Proofpoint Messaging Security Gateway, and to encourage customers, users and developers to use HackAlert Code Secure, Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection Server, and Proofpoint Messaging Security Gateway and practice the methods taught in the '305 Patent.

115. Defendants have had knowledge of the '305 Patent at least as of the time they learned of this action for infringement, and by continuing the actions described above, Defendants have had the specific intent to or was willfully blind to the fact that their actions would induce infringement of the '305 Patent.

COUNT IX
(Direct Infringement of the '408 Patent pursuant to 35 U.S.C. § 271(a))

116. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

117. Defendants have infringed and continues to infringe one or more claims of the '408 Patent in violation of 35 U.S.C. § 271(a).

118. Defendants' infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

119. Defendants' acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

120. Defendants' infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendants' products and services, including but not limited to, Proofpoint Zero-Hour and CodeSecure, which embody the patented invention of the '408 Patent.

121. As a result of Defendants' unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

122. Defendants' infringement of the '408 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT X
(Indirect Infringement of the '408 Patent pursuant to 35 U.S.C. § 271(b))

123. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

124. Defendants have induced and continue to induce infringement of at least claims 1-8 and 23-28, of the '408 Patent under 35 U.S.C. § 271(b).

125. In addition to directly infringing the '408 Patent, Defendants indirectly infringe the '408 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to its customers, users and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '408 Patent, where all the steps of the method claims are performed by either Defendants or their customers, users or developers, or some combination thereof. Defendants have known or have been willfully blind to the fact that they are inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendants, one or more method claims of the '408 Patent.

126. Defendants knowingly and actively aid and abet the direct infringement of the '408 Patent by instructing and encouraging their customers, users and developers to use Proofpoint Zero-Hour and CodeSecure. Such instructions and encouragement include, but are not limited to, advising third parties to use Proofpoint Zero-Hour and CodeSecure in an infringing manner; providing a mechanism through which third parties may infringe the '408 Patent, specifically through the use of the Proofpoint Zero-Hour and CodeSecure; advertising and promoting the use of the Proofpoint Zero-Hour and CodeSecure in an infringing manner; and distributing guidelines and instructions to third parties on how to use the Proofpoint Zero-Hour and CodeSecure in an infringing manner.

127. Defendants provide detailed instructions to their customers and users regarding all aspects of the Proofpoint Zero-Hour and CodeSecure including HackAlert Code Secure, Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection Server, and Proofpoint Messaging Security Gateway. Examples of these instructions can be found at the Armorize Resource Center (at http://armorize.com/index.php?link_id=product), Armorize Forums / Tutorials, FAQs (at

https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources), and Proofpoint Resources (at http://www.proofpoint.com/resources/index.php).

128. Proofpoint itself and through its authorized partners regularly provide class-room style training, demonstrations, webinars, and certification programs to help users use Proofpoint Targeted Attack Protection and Malware Analysis Service including without limitation the following:

- Webinars on Contextual Security Approach to Protection From Targeted Threats, Undetected Threats: Finding and protecting against hundreds of missed attacks, Combatting 2013's Most Dangerous Attacks, and Spearing the Spear Phishers: How to Reliably Defeat Targeted Attacks. *See* http://www.proofpoint.com/resources/webinars.php (attached as Exhibit Q);

- Demonstrations including Proofpoint Integrated Product Suite Demo and Proofpoint Enterprise Protection Live Demo. The demonstrations show how to use the Targeted Attack Protection to protect organizations. *See* http://www.proofpoint.com/resources/demos.php (attached as Exhibit R);

- Technical Briefs on Proofpoint Zero-Hour Anti-Virus and White Papers on Targeted Attack: The Best Defense, Defense against the Dark Arts: Finding and Stopping Advanced Threats, and Longline Phishing: A New Class of Advanced Phishing Attacks. *See* http://www.proofpoint.com/resources/white-papers.php (attached as Exhibit S);

- Proofpoint Education Portal, which offers courses in Enterprise Protection, Accredited Engineer, Enterprise Protection Suite, Enterprise Protection for the Administrator, Proofpoint Targeted Attack Protection for End Users, Staying Safe on E-mail, and Enterprise Protection Associate Level Training. *See* http://www.training.proofpoint.com/courses-draft/ (attached as Exhibit T);

- Proofpoint Education Portal which offers On-Site Training where a group of up to 8 people can be trained live by Proofpoint to use their Protection products. *See* http://www.training.proofpoint.com/classroom-schedule/on-site/ (attached as Exhibit U).

129. Proofpoint offers Professional Services, which helps customers design and implement Proofpoint's products onto the customers' network. Professional Services also offers integration, customization, training and maintenance of Proofpoint's products.

130. Armorize posts tutorials, user guides, troubleshooting and explanation on how to use Armorize technology on its online forum. These include without limitation documents on

CodeSecure Quick Start Guides, How to upgrade CodeSecure, and LDAP integration tip with CodeSecure. *See* https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources (attached as Exhibit V).

131. Defendants actively and intentionally maintain and update websites, including Proofpoint.com and Armorize.com, to promote and provide demonstration, instruction and technical assistance for HackAlert Code Secure, Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection Server, and Proofpoint Messaging Security Gateway, and to encourage customers, users and developers to use HackAlert Code Secure, Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials (including the packages of Beginner, Business, and Professional), Proofpoint Protection Server, and Proofpoint Messaging Security Gateway products and practice the methods taught in the '408 Patent.

132. Defendants have had knowledge of the '408 Patent at least as of the time they learned of this action for infringement, and by continuing the actions described above, Defendants have had the specific intent to or was willfully blind to the fact that their actions would induce infringement of the '408 Patent.

COUNT XI
(Direct Infringement of the '086 Patent pursuant to 35 U.S.C. § 271(a))

133. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

134. Armorize has infringed and continues to infringe one or more claims of the '086 Patent in violation of 35 U.S.C. § 271(a).

135. Armorize's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

136. Armorize's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

137. Armorize's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Armorize's products and services, including but not limited to, the HackAlert and CodeSecure, which embody the patented invention of the '086 Patent.

138. As a result of Armorize's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

139. Armorize's infringement of the '086 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT XII
(Indirect Infringement of the '086 Patent pursuant to 35 U.S.C. § 271(b))

140. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

141. Armorize has induced and continues to induce infringement of at least claims 1-8, 17-23, 31, 32, 35, 36, 39, and 41 of the '086 Patent under 35 U.S.C. § 271(b).

142. In addition to directly infringing the '086 Patent, Armorize indirectly infringes the '086 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to its customers, users and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '086 Patent, where all the steps of the method claims are performed by either Armorize or its customers, users or developers, or some combination thereof. Armorize has known or has been willfully blind to the fact that it is inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Armorize, one or more method claims of the '086 Patent.

143. Armorize knowingly and actively aided and abetted the direct infringement of the '086 Patent by instructing and encouraging its customers, users and developers to use HackAlert and CodeSecure. Such instructions and encouragement include but are not limited to, advising third parties to use HackAlert and CodeSecure in an infringing manner; providing a mechanism through which third parties may infringe the '086 Patent, specifically through the use of HackAlert and CodeSecure; advertising and promoting the use of HackAlert and CodeSecure in an infringing manner; and distributing guidelines and instructions to third parties on how to use HackAlert and CodeSecure in an infringing manner.

144. Armorize provides detailed instruction to its customers and users regarding all aspects of HackAlert and CodeSecure including, HackAlert, HackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, and HackAlert Vulnerability Assessment, SmartWAF, and HackAlert CodeSecure. Examples of these instructions can be found at the Armorize Resource Center (at http://armorize.com/index.php?link_id=product), Armorize Forums / Tutorials, FAQs (at https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources), and Proofpoint Resources (at http://www.proofpoint.com/resources/index.php).

145. Armorize posts tutorials, user guides, troubleshooting and explanation on how to use Armorize technology, including CodeSecure and HackAlert, on its online forum. These include without limitation documents on CodeSecure Quick Start Guides, How to upgrade CodeSecure, and LDAP integration tip with CodeSecure. *See* https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources (attached as Exhibit V).

146. Armorize also posts tutorials, user guides, troubleshooting and explanation on how to use HackAlert on its online forum. These include HackAlert Resources, HackAlert SafeImpression question documents, tutorials on what to do "when a drive-by-download knocks at your door,"

tutorial on "How to add a website into HackAlert to be monitored," and tutorial on "what to do when receiving an alert." *See* https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources (attached as Exhibit V).

147. Armorize Provides the HackAlert V5 API, which encourages developers and customers to use HackAlert with step-by-step instructions on how to integrate into the HackAlert Software. *See* Armorize Malware Scanning and Forensics Extraction API (attached as Exhibit P).

148. Armorize actively and intentionally maintains and updates websites, including Armorize.com, to promote and provide demonstration, instruction and technical assistance for HackAlert and CodeSecure, and to encourage customers, users and developers to use HackAlert and CodeSecure products and practice the methods taught in the '086 Patent.

149. Armorize has had knowledge of the '086 Patent at least as of the time it learned of this action for infringement, and by continuing the actions described above, Armorize has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '086 Patent.

COUNT XIII
(Direct Infringement of the '154 Patent pursuant to 35 U.S.C. § 271(a))

150. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

151. Armorize has infringed and continues to infringe one or more claims of the '154 Patent in violation of 35 U.S.C. § 271(a) since the issuance of the Certificate of Correction.

152. Armorize's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

153. Armorize's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

154. Armorize's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Armorize's products and services, including but not limited to, the HackAlert and CodeSecure, which embody the patented invention of the '154 Patent.

155. As a result of Armorize's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

156. Armorize's infringement of the '154 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT XIV
(Direct Infringement of the '918 Patent pursuant to 35 U.S.C. § 271(a))

157. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

158. Armorize has infringed and continues to infringe one or more claims of the '918 Patent in violation of 35 U.S.C. § 271(a).

159. Armorize's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

160. Armorize's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

161. Armorize's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Armorize's products and services, including but not limited to, HackAlert and CodeSecure, which embody the patented invention of the '918 Patent.

162. As a result of Armorize's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

163. Defendant's infringement of the '918 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT XV
(Indirect Infringement of the '918 Patent pursuant to 35 U.S.C. § 271(b))

164. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

165. Armorize has induced and continues to induce infringement of at least claims 1-11, 22-28, and 34 of the '918 Patent under 35 U.S.C. § 271(b).

166. In addition to directly infringing the '918 Patent, Armorize indirectly infringes the '918 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to its customers, users and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '918 Patent, where all the steps of the method claims are performed by either Armorize or its customers, users or developers, or some combination thereof. Armorize has known or has been willfully blind to the fact that it is inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Armorize, one or more method claims of the '918 Patent.

167. Armorize knowingly and actively aids and abets the direct infringement of the '918 Patent by instructing and encouraging its customers, users and developers to use HackAlert and CodeSecure. Such instructions and encouragement include but are not limited to, advising third parties to use HackAlert and CodeSecure in an infringing manner; providing a mechanism through which third parties may infringe the '918 Patent, specifically through the use of HackAlert and CodeSecure; advertising and promoting the use of HackAlert and CodeSecure in an infringing manner; and distributing guidelines and instructions to third parties on how to use HackAlert and CodeSecure in an infringing manner.

168. Armorize provides detailed instruction to its customers and users regarding all aspects of HackAlert and CodeSecure, including: HackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, and HackAlert Vulnerability Assessment, SmartWAF, and HackAlert CodeSecure. Examples of these instructions can be found at the Armorize Resource Center (at http://armorize.com/index.php?link_id=product), and Armorize Forums / Tutorials, FAQs (at https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources).

169. Armorize posts tutorials, user guides, troubleshooting and explanation on how to use Armorize technology, including CodeSecure, on its online forum. These include documents on CodeSecure Quick Start Guides, How to upgrade CodeSecure, and LDAP integration tip with CodeSecure. *See* https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources (attached as Exhibit V).

170. Armorize also posts tutorials, user guides, troubleshooting and explanation on how to use HackAlert on its online forum. These include HackAlert Resources, HackAlert SafeImpression question documents, tutorials on what to do "when a drive-by-download knocks at your door," tutorial on "How to add a website into HackAlert to be monitored," and tutorial on "what to do when receiving an alert." *See* https://armorize.zendesk.com/categories/5972-Tutorials-FAQs-Resources (attached as Exhibit V).

171. Armorize provides the HackAlert V5 API, which encourages developers and customers to use HackAlert with step-by-step instructions on how to integrate into the HackAlert Software. *See* Armorize Malware Scanning and Forensics Extraction API (attached as Exhibit P).

172. Armorize actively and intentionally maintains and updates websites, including Armorize.com, to promote and provide demonstration, instruction and technical assistance for

HackAler and CodeSecure, and to encourage customers, users and developers to use HackAlert and CodeSecure products and practice the methods taught in the '918 Patent.

173. Armorize has had knowledge of the '918 Patent at least as of the time it learned of this action for infringement, and by continuing the actions described above, Armorize has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '918 Patent.

PRAYER FOR RELIEF

WHEREFORE, Finjan prays for judgment and relief as follows:

A. An entry of judgment holding that Defendants have infringed and are infringing the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent, the '154 Patent and the '918 Patent; and that Defendants have induced and are inducing infringement of the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent and the '918 Patent;

B. A preliminary and permanent injunction against Defendants and their officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing, or inducing the infringement of, the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent, the '154 Patent and the '918 Patent and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

C. An award to Finjan of such damages as it shall prove at trial against Defendants that is adequate to fully compensate Finjan for Defendants' infringement of the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent, the '154 Patent and the '918 Patent, said damages to be no less than a reasonable royalty;

D. A finding that this case is "exceptional" and an award to Finjan of its costs and reasonable attorney's fees, as provided by 35 U.S.C. § 285;

E. An accounting of all infringing sales and revenues, together with postjudgment interest and prejudgment interest from the first date of infringement of the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent, the '154 Patent and the '918 Patent;

F. Such further and other relief as the Court may deem proper and just.

Respectfully submitted,

Dated: November 21, 2014

By: */s/ Paul J. Andre*

Paul J. Andre
Lisa Kobialka
James Hannah
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Plaintiff
FINJAN, INC.

DEMAND FOR JURY TRIAL

Finjan demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: November 21, 2014

By: */s/ Paul J. Andre*

Paul J. Andre
Lisa Kobialka
James Hannah
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Plaintiff
FINJAN, INC.